



Nieuwsbrief 358

The new front line: how cybercrime-as-a-service affects the future of warfare

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

De nieuwe frontlinie: hoe cybercrime-as-a-service de toekomst van oorlogsvoering beïnvloedt

In de wereld van vandaag is digitale oorlogsvoering geen toekomstscenario meer maar realiteit. Met de opkomst van Cybercrime-as-a-Service is het speelveld fundamenteel veranderd. Criminelen zonder technische kennis kunnen nu eenvoudig krachtige cyberaanvallen uitvoeren door deze als dienst in te kopen. Wat betekent dit voor onze veiligheid en hoe groot is de rol van Telegram en het darkweb hierin? Dit artikel werpt een scherp licht op deze verontrustende ontwikkelingen en laat zien waarom waakzaamheid geen keuze meer is maar noodzaak.

[Lees verder](#)

The changing DNA of organized crime and its impact on digital threats

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

De veranderende DNA van georganiseerde misdaad en de impact op de digitale dreigingen

De aard van georganiseerde misdaad verandert ingrijpend. Waar criminele netwerken vroeger vooral fysiek opereerden, verschuift hun speelveld steeds meer naar de digitale ruimte. Technologie en geopolitiek geven deze ontwikkeling extra vaart, waardoor de impact op onze veiligheid toeneemt. In dit artikel ontdek je hoe deze netwerken zich aanpassen aan het digitale tijdperk en welke dreigingen daaruit voortkomen voor onze samenleving.

[Lees verder](#)

DDoS attacks in the context of cyberwar: New threats and defense strategies for 2025

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

DDoS-aanvallen in de context van cyberoorlog: Nieuwe dreigingen en verdedigingsstrategieën voor 2025

De dreiging van DDoS-aanvallen ontwikkelt zich razendsnel en speelt een steeds grotere rol binnen de context van geopolitieke spanningen en digitale oorlogsvoering. In dit artikel ontdek je hoe deze aanvallen in 2025 niet alleen sneller en complexer worden, maar ook hoe kunstmatige intelligentie een cruciale rol speelt in zowel de aanval als de verdediging. Wat betekent dit voor organisaties die hun digitale weerbaarheid willen versterken? Lees verder en krijg inzicht in de nieuwste dreigingen en slimme verdedigingsstrategieën die nodig zijn om voorop te blijven lopen in een steeds vijandiger digitaal landschap.

[Lees verder](#)

Question of the week: why is NIS2 important to your business and how do you handle it?

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Vraag van de week: Waarom is NIS2 belangrijk voor jouw bedrijf en hoe ga je ermee om?

De Europese NIS2-richtlijn zet cybersecurity definitief op de kaart, ook voor het midden en kleinbedrijf. Waar veel ondernemers denken dat deze regels alleen gelden voor grote organisaties, toont de praktijk iets anders. Lever je diensten aan grotere partijen of ben je onderdeel van een toeleveringsketen, dan is de kans groot dat NIS2 ook voor jouw bedrijf gevolgen heeft. In dit artikel lees je waarom NIS2 belangrijk is voor jouw organisatie en hoe je je hierop kunt voorbereiden.

[Lees verder](#)

The rise of privacy coins on the darkweb: Bitcoin gives way to anonymous trading

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

De opkomst van privacy coins op het darkweb: Bitcoin maakt plaats voor anoniem handelen

Terwijl Bitcoin jarenlang het betaalmiddel bij uitstek was op het darkweb, maken steeds meer criminelen de overstap naar privacy coins zoals Monero en Zcash. Deze digitale valuta bieden een mate van anonimiteit die Bitcoin simpelweg niet kan evenaren. Maar wat betekent deze verschuiving voor de aanpak van cybercriminaliteit en de opsporing van illegale activiteiten? In dit artikel duiken we in de opkomst van privacy coins en stablecoins op het darkweb en laten we zien hoe dit het speelveld van zowel criminelen als wetshandhavers ingrijpend verandert.

[Lees verder](#)

De opsporingstiplijn: 0800-6070

Zaaknummer Politie: 2024213772 - Sas van Gent

[Reading in another language](#)

Sas van Gent - Helpdesk fraude

Een jongeman pint in Sas van Gent met een bankpas die via oplichting is buitgemaakt en verdwijnt daarna spoorloos. De politie vermoedt dat hij minderjarig is en geeft hem tot 7 maanden de tijd om zich te melden voordat zijn gezicht herkenbaar wordt getoond. In dit artikel leest u hoe deze vorm van helpdeskfraude werkt en waarom alertheid op vishing, smishing en tech support scams belangrijker is dan ooit. Herkent u de signalen van digitale oplichting? Ontdek hoe u zichzelf en anderen kunt beschermen.

[Lees verder](#)

AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De **AI HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over verschillende aspecten van HRM binnen de politie.

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer, In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een onafhankelijke en betrouwbare bron van informatie**
Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
- **Bewustwording en preventie mogelijk maken**
Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Met vriendelijke groet,
Het team van Cybercrimeinfo



Doneer | Cybercrimeinfo.nl | ccinfo.nl

Doneer pagina

Geen budget? Geen probleem! Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.

Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review**.

Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol! Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo (ccinfo)

Schrijf een review



Share



Tweet



Share



Pinterest



Bluesky



Mastodon

Deze e-mail is verstuurd aan {{email}}.

Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#).

U kunt ook uw [gegevens inzien en wijzigen](#).

Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.